Perceptions and actions: Combining privacy and risk perceptions to better understand user behaviour

Lynne Coventry
PaCT Lab, Psychology Dept.
Northumbria University
Newcastle-upon-Tyne, UK
lynne.coventry@northumbria.ac.uk

Debora Jeske
PaCT Lab, Psychology Dept.
Northumbria University
Newcastle-upon-Tyne, UK
debora.jeske@northumbria.ac.uk

Pam Briggs
PaCT Lab, Psychology Dept.
Northumbria University
Newcastle-upon-Tyne, UK
p.briggs@northumbria.ac.uk

ABSTRACT
Exploring the link between privacy and behaviour has been difficult, as many contextual and other variables lead to a schism between privacy attitudes and behaviour. We propose that one possible means forward is to consider risk perceptions as an important additional dimension when exploring individual differences in privacy concern. Using cluster analysis, we demonstrate the benefit of creating more multi-dimensional user profiles (=clusters) as these can provide a better inside into behaviour. These clusters were able to differentiate users based on both privacy and risk perceptions into users who were (a) highly concerned and risk-sensitive; (b) unconcerned but risk-aware; and (c) moderately concerned but less risk-aware cluster. Using these clusters, we were able to explain different patterns of self-reported behaviours related to technical and general caution. Further analysis of behaviours associated with the use of mobile devices, public networks and social networking in relation to these clusters did not result in any significant findings. We provide a number of topics for discussion and practical solutions that have yet to be implemented in order to better understand the link between privacy attitudes and behaviour.

1. INTRODUCTION
Underlying the wide ranging discussions on privacy is a general agreement that privacy is desirable and beneficial, and in fact we have a legally protected right to privacy. Privacy is also a commodity that people are prepared to trade, e.g. in order to receive personalized recommendations. However, there is little agreement on what exactly privacy means. Privacy has been defined as "'the claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [26]. Privacy can also be considered separate from the public domain, which is voluntary and temporary and free from intrusion. The experience of privacy provides relief from stressors and opportunities for personal development, both of which are crucial to the well-being of the individual [20]. However, privacy does not necessarily mean complete withdrawal from interaction or refusing to share information; rather the "selective control of access" [1; 8]. This allows the level of privacy to be optimized in different situations.

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11,

A number of critical issues unite privacy, self-disclosure and technology use: lack of knowledge of how information will be used, perceived control over that use, trust and vulnerability and perceived costs and benefits [14; 19], and how technological advances led to loss of reserve [10]. We trade reserve for many different things including loyalty points, or to brag about where we are. While we are increasingly giving away information we are also increasingly losing control of the dissemination of the information and have little control over who has access to that information. This is in part facilitated by new devices and the federated network of applications that may have access to personal data. For this, and other reasons, mobile devices such as smartphones are still considered more problematic in terms of the privacy they provide when compared to other mobile devices such as laptops [4].

1.1 Linking privacy and behaviour
Privacy attitudes do not always predict privacy behaviours and this can be explained with reference to a variety of research studies. We would like to focus on behaviours involving some form of security risk, in part because insecure behaviours are those most likely to create privacy vulnerabilities. So why are privacy preferences and privacy or security behaviours sometimes at odds?

First, privacy perceptions are themselves complex and dynamic – showing different kinds of contextual dependency. Six different types of privacy have been proposed [21], each outlining an area over which people wish to have control over; family intimacy friends intimacy, solitude, isolation, anonymity and reserve. This suggests that different types of privacy may be relevant in different circumstances.

Second, privacy attitudes may not translate into associated behaviours due to a range of other, more pressing personal beliefs and (mis)perceptions (e.g., [4; 13]). Beliefs can and do influence decisions, but these beliefs may themselves be based upon a socially constructed model of what constitutes a security threat [17]. In addition, people may not even consider their privacy concerns when making certain security decisions [13; 16]. We conducted a variety of interviews with users of mobile devices. We found that many non-experts are aware of the discrepancy between privacy concerns and their actions (manuscript in preparation). At the same time, many individuals seemed to be unaware of what types of behaviours place them at risk and may actually cause or lead to privacy violations. These explanations were often based on personal perceived competence (akin to "I don't do that") and knowledge of risky behavioural choices (like

"I recognize dodgy emails"). This means privacy concern may not relate or translate into specific behavioural actions because the user does not realize that his or her actions are actually in conflict with his or her privacy concerns [16].

Third, individuals may underestimate the consequences of their actions – indeed, few realize just how much personally identifying and sensitive information they share online (e.g., [16]), potentially with strangers when not adapting their personal settings on social networks. In addition, they may not realize that games and apps accessible via social networks are not vetted for security although they appear to be an integral part of the social network which has clear privacy settings [15].

Fourth, some actions need to be primed. That is, no action may be deemed necessary by a user until a significant privacy violation occurs. Critical privacy-and security-related events can have a behavioural effect on the organization as a whole (in terms of changed policies, see example in [5]) or individual behaviour [15]. For example, previous experience of privacy violation on social networks can predict privacy attitudes [15]. This suggests that privacy attitudes within organizations and individuals may be subject to critical incidents. Unfortunately, the effect of these incidents – in line with the availability heuristic – may be short-lived.

1.2 Privacy concern in relation to risk

We believe that one of the reasons why privacy is not always related to behaviour relates to the multi-dimensional nature of privacy (see types in [21]) which may not be readily separated from perceptions of risk, as these may encourage more active or passive reactions on the part of the user in response to heightened privacy concerns.

Several example help explain how both privacy and perceptions of risk may relate to each other. One explanation put forward is that perceived risk can have a significant negative on online behaviour, even though privacy-active behaviour does not [6]. Research results suggest that privacy concerns may be differentiated in terms of the extent to which privacy is linked to awareness of risks, suspicion about potentials risks being involved, and active privacy-promoting behaviours [6]. This again proposes a link between privacy concern and risk behaviour. Willingness to provide personal information may be in part influenced by users' concerns or fears that this data is misused [27]. The framework of online information privacy research by [18] also recognizes perceived risks and threats to one's privacy are important elements informing individual's need for privacy.

1.3 Research goals

We wanted to contribute to the better understanding of the literature by considering a more multi-dimensional approach to how we examine privacy-related behaviours by allowing for privacy to be considered in combination with risk perceptions.

Our research pursued two different goals. In the first instance we wanted to generate a more multi-dimensional typology of users that rested not just on privacy concern alone, but also incorporate other perceptions that link to privacy. This means, rather than starting to predict privacy types or concerns, we used user perceptions of risk associated to their privacy and data as a starting point to differentiate users. Using cluster analysis, we created three clusters of users. Each cluster differed significantly from each other in terms of their privacy concern, perceived vulnerability to risk and severity of risk.

The next research goal was to examine the utility of creating a new typology of users based on perceptions to examine actual behaviours. We wanted to find out if these more multi-dimensional user clusters could help us better understand user behaviours in relation to specific behaviours. These behaviours included general and technical caution, the selection of secure vs. open public wireless network options, use of wireless to access social networks.

2. METHOD

In the following section, we describe our measures and procedures.

2.1 Measures

We were interested in assessing the relationship between privacy concerns, perceived vulnerability to risk, perceived severity of risk, technical and general caution, the use of wireless networks, social networks. In order to measure actual behaviours in addition to self-report, we also a small decision-making part, where participants had to choose one of six public wireless network options to connect to across five different screens. This meant that the behavioural measures included both self-reported behaviours and actual behavioural decisions made by participants.

2.1.1 Perceptions of risk and privacy concern

We used three items derived from the original 16-item scale introduced by [3] to measure privacy concern. The original scale had included questions not statements, each with response options on a five-point scale ranging from "not at all" to "very much" (α=.74, =2.40, SD=.93). Perceived vulnerability to risk was measured using four items from [12]. We changed the response scales to a five-point scale ranging from "extremely low" to "extremely likely" (α=.83, MN=3.05, SD=.72). Perceived severity was measured using three items from [12]. We changed the response scales to a five-point scale ranging from "strongly disagree" to "strongly agree" (α=.85, MN=4.05, SD=.87). The subscales all correlated positively ($r>.3$, $p\leq.002$).

2.1.2 Self-reported behaviour

Technical caution was measured using four items from the technical privacy behaviour scale by Buchanan et al (2007). A couple of example behaviours were: "Do you check your computer for spy ware?" and "Do you remove cookies?" The five-point response scale ranging from "never" to "always" (α=.67, MN=3.16, SD=.79). General caution was measured using one item ("Do you destroy (burn or shred) your personal documents when you are disposing of them?", also by [3] and the same response scale (MN=3.21, SD=1.37).

Additional self-reported behaviours of interest included the frequency of public wireless networks and social networking sites. The questions were as follows: (a) "How frequently do you connect your devices (work iPad, tablet, laptop) to a public wireless network?" and (b) "How likely are you to use your mobile devices to access social networking sites (e.g., Facebook, Twitter, MySpace, Instagrams, LinkedIn, YouTube, etc.)?" The response options were identical for both questions: (1) daily, (2) weekly, (3) monthly, (4) less than once a month, and (5) never.

2.1.2 Other behavioural outcomes

We presented all participants with five different screenshots, each featuring six different wireless network options (secure and unsecure/open options). This gave us a measure on a restricted range (0-5) for the overall frequency with which secure and open networks were selected.

2.2 Procedure

We recruited 104 social science students to participate in a survey. While the questionnaire part involved self-report, the decision-making task involved a small vignette. All participants were given the following scenario: they have an hour to submit some urgent work and decide to go to a public café to connect to the Internet. In this context, they are presented with various network options. Participants were then asked to indicate their first choice from the available options on the five screen shots and to explain why they had picked specific networks in order to examine which features were effective. These explanations suggested that trusted implied secure for almost all participants. All images were randomly presented to reduce order effects.

All participants could earn research credits for their respective programs. All students could register for the study online. No inclusion or exclusion criteria were posited as the recruitment sample was believed to be an ideal target audience. All potential recruits would be social science rather than computing science students (to avoid ceiling effects). In addition, we believed that we had a representative sample of wireless network users with varying levels of IT proficiency. As we used coloured display, we excluded one participant who indicated that he was colour-blind (N=104).

3. RESULTS

3.1 Privacy and risk perceptions

We decided to examine whether or not our participants fell into specific types of clusters of individuals that share different degrees of concern about their privacy and risk. We wanted to use these clusters as a better means to better interpret privacy behaviours (general and technical caution), social networking behaviour, and use of public networks via mobile devices.

In order to determine these groups in the larger dataset (N=104), we decided to utilize hierarchical cluster analysis [9]. We used the responses we had retained for three subscales (privacy concern, perceived severity of risk, and perceived vulnerability). Each of these scales featured five response options (frequency for privacy, agreement scales for perceived severity and vulnerability to risk). We applied a hierarchical cluster analysis using Ward's (1963) linkage method, using the squared Euclidean distance as a measure of similarity [25]. The visualization of the clustering process in the dendrogram indicated two possible solutions, namely two or four groups of classifications. We analysed the group sizes of the four-factor solution (n_1=26, n_2=39, n_3=32, and n_4=7). All analyses of variance involving the three subscale composites (for privacy concern, perceived severity and vulnerability to risk) indicated significantly different group means. However, given that the fourth cluster was so small, we used the original four cluster solution to generate a new cluster variable – this time excluding all cases that fell into the fourth category. This therefore generated a three-category variable in a new dataset of 97 cases which we used to examine group differences.

3.2 Description of cluster characteristics

The clusters can be differentiated as follows (see Table 1 for details). The first cluster appeared to have the highest concern for their privacy (3.37). This seems to coincide with higher scores on the perceived severity of risk (4.63), indicating a much higher degree of concern about others having access to their data. This group also had a strong sense that they are more likely to be vulnerable to risks (3.72). As a result, we labelled this first group as the *highly concerned and risk-sensitive cluster*.

The second cluster has very low privacy concerns (1.76). They are also not feeling particularly vulnerable, that is, they are not as concerned about risks affecting them (2.58). They do, however, indicate a moderate level of perceived severity of risk (4.23). This suggests that they recognize the seriousness of various threats for their data. We named this cluster the *unconcerned but risk-aware cluster*.

The third cluster were moderately concerned about their privacy (2.54) and considered themselves somewhat vulnerable to risk (3.30). They were not as concerned as the other two clusters about potential threats having a serious effect on them. This means, their perceived severity of risk was lowest amongst the three groups (3.76). Based on these characteristics, this cluster is the *moderately concerned but less risk-aware cluster.* In the next step, we wanted to test if we can use our multi-dimensional clusters to better understand and interpret security-related behaviours.

Table 1: Cluster characteristics

Scales	Cluster 1 (n=26) M (SD)	Cluster 2 (n=39) M (SD)	Cluster 3 (n=32) M (SD)	Analysis of variance
Privacy concern	3.37 (.85)	1.76(.59)	2.54(.63)	$F(2,94)=44.204$, $p<.001$
Perceived severity of risk	4.63 (.42)	4.23(.60)	3.76(.60)	$F(2,94)=17.387$, $p<.001$
Perceived vulnerability to risk	3.72 (.42)	2.58 (.52)	3.30 (.49)	$F(2,94)=45.83$, $p<.001$

Note. N_{red}=97. Post-hoc analysis between the three groups indicated significant group differences across the board for privacy concern ($p<.001$), perceived severity of risk ($p\leq.018$), and perceived vulnerability to risk ($p\leq.005$). These results remained identical if we considered the role of age and gender. Cluster labels: 1 = highly concerned and risk-sensitive cluster; 2= unconcerned but risk-aware cluster; 3= moderately concerned but less risk-aware cluster.

3.3 Cluster differences in behaviours

We were interested in how well our multi-dimensional clusters could help explain different behaviours. These were: general and technical caution, the selection of secure vs. open public wireless network options, use of wireless to access social networks.

3.3.1 Technical caution (self-reported)

We first examined technical caution. Using ANOVA (gender and age were not significant covariates), we wanted to examine if the extent to which our participants engaged in behaviours related to technical caution would be different across the three clusters we determined. This was indeed the case ($F(2,94)=4.025$, $p=.021$, partial $\eta^2 = .08$).

However, the differences between the clusters seem to be most pronounced and between those in cluster 1 (*highly concerned and risk-sensitive*) compared to those in cluster 2 (*unconcerned but risk-aware*) and in relation to cluster 3 (*moderately concerned but less risk aware*). Post-hoc analysis suggested that these group comparisons were all statistically significant ($p>.05$). No difference emerged between cluster 2 and 3 (p=ns). Descriptives suggest that those who were *highly concerned about privacy and risk sensitive* (cluster 1) also tended to report a greater average of behaviours related to technical caution (MN=3.49, SD=.78) than those who were u*nconcerned and risk aware* (cluster 2, MN=2.99, SD=.71) or *moderately concerned but less risk aware* (cluster 3, MN=2.99, SD=.81). The descriptives are pictured in Figure 1. The vertical axis refers to the technical caution (a higher scores indicates greater frequency with which individuals removed cookies, checked for spyware and similar).

3.3.2 General caution (self-reported)

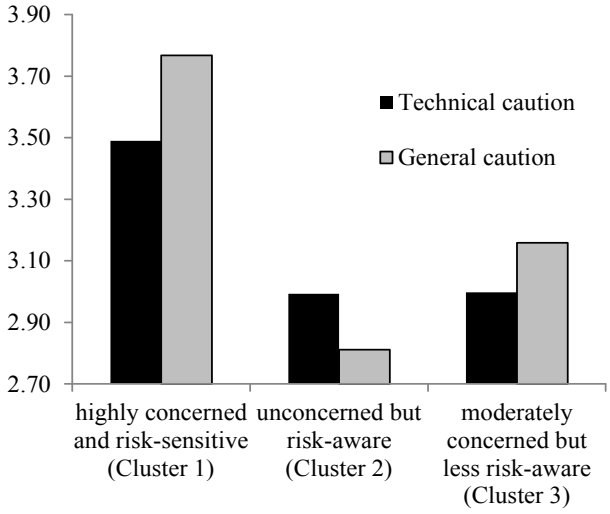
We first examined general caution. Again, using ANCOVA (age was a significant covariates, $p=.015$), we observed a significant differences between the clusters ($F(2,87)=3.460$, p=.036, partial $\eta^2 = .07$, n=91). A significant difference arose between those in cluster 1 (highly concerned and risk-sensitive) compared to those in cluster 2 (unconcerned but risk-aware) as indicated in the post-hoc analysis ($p=.031$). No other significant group differences arose.

Descriptives suggest that those who were highly concerned about privacy and risk sensitive (cluster 1) would more often destroy personally identifiable information (MN=3.77, SD=1.21) than those who were unconcerned yet risk aware (cluster 2, MN=2.81, SD=1.46) or moderately concerned but less risk aware (cluster 3, MN=3.16, SD=1.32). The weak but positive correlation with age suggested that older participants would be more likely to dispose of their documents carefully ($r=.262$, $p=.009$). The results for technical and general caution are listed next to one another in Figure 1.

3.3.3 Selection of wireless networks

We also wanted to examine if our clusters could help explain which types of open wireless networks our participants selected. We did not observe any significant group differences. The different clusters did not differ significantly in terms of the extent to which they selected fewer or more open networks when connecting to public wireless. The same applies to the extent to which they selected secure networks.

Figure 1. Technical and general caution amongst different clusters



Note. The y-axis refers to the average score obtained in terms of technical and general caution. Higher scores indicate that participants would more frequently engage in behaviours associated with technical and caution.

3.3.4 Use of social networks and public wireless networks (self-reported)

We observed no significant differences in relation to the frequency with which the three clusters accessed social networks or public wireless. This indicates that in our sample, decisions about social networks and the use of public wireless must be driven by other variables – those not immediately related to privacy concerns.

4. DISCUSSION

The results of our survey can be summarized as follows. The use of multiple scales to produce multi-dimensional clusters seemed to be useful tool when interpreting behaviours related to technical and general caution. The differentiated findings suggest that privacy concern, even when moderately high, will not result in the same behaviours compared to privacy concern that is also combined with great risk concern.

The different responses of the clusters in terms of general and technical caution also link to findings by [13]. These authors found very different subgroups, who while concerned about personal privacy, also utilized very different decision-making strategies. In our case, we see that the combination of concerns (privacy and risk) is what drives behaviours. This gives credence the benefit of considering multiple user variables when trying to analyse behaviour, particularly privacy behaviour.

Privacy concerns may not predict all behaviours, when these are security related (see also [4]). When we considered alternative behaviours, the picture quickly became murky. The actual use of certain devices or online services seems to be a function of other variables not included in our survey. We believe that these behaviours may depend on the situation and devices that individuals have at their disposal. Previous work suggests that

behaviours such as installing new free applications will depend on the type of devices the person is using [4]. Smaller mobile devices such as smartphones may be used as secondary devices that users are also more comfortable using to try out new applications (even though such behaviours may be in conflict with their privacy concerns).

This brings us to the limitations of our work. Surveys are best suited for attitudinal assessments, rather than behaviours or experience [13]. Unfortunately, much of the research on privacy and behaviour suffers from the short-coming. Our study is no different. The use of self-report (in relation to social networking) and insufficient external validity of the network selection task may have impacted our results, even though we made sure to use Android default screens when presenting the network options. These circumstances limit the possible generalizability of our findings.

There is still considerable ambiguity in our understanding of privacy within the technology domain, and there has been little systematic research exploring privacy aspects related to the sharing of location information, preferences, and habits from and between supportive/assistive technologies by older adults. We hope we made a small contribution by helping to provide a more multi-dimensional picture of how user behaviour may be influenced by a combination of privacy and risk perceptions.

5. WORKSHOP QUESTIONS AND CONTRIBUTION

Our results suggest that privacy concerns may be complemented by risk perceptions to better understand behavioural outcomes. In addition to the methodological contribution, we believe that our research experience may be relevant in the discussion of the following themes and queries:

How can we increase user understanding of privacy-related risks associated with prevalent and risky behaviours?

One suggestion is to develop a user-centric security maturity model that consider user's privacy concerns for different parts of their data, their knowledge about how their behaviour can compromise their privacy. One issue here is that many users may not understand, read EULA and process the details in these policies (e.g.,[15]). At the same time, purchases are considered giving consent to consumer data being used for other purposes, even when the consumers will not have formally read nor agreed to the privacy policy of the company (see [13]).

If we can make smoking warning labels easier to understand, why is this not being done in IT? We need to redefine what are "fair information practices" [11]. Moreover, when online websites feature more salient privacy information about how they protect the consumer's data, potential consumers were also more likely to pay a premium to purchase products from these sites [24]. This demonstrates salience can be beneficial. Further suggestions are outlined in [13]

In addition, it is important to question the idea that digital natives will automatically understand technology (see also [16]) and employ more than just basic safeguards (e.g., [7]). Some evidence actually suggests that the younger users are less concerned about privacy threats than younger users of social networks [11].

But even if we increase user understanding, any intervention also needs to increase user motivation and interest to protect themselves and their data more carefully. Recommendations vary, ranging from making users take more responsibility (e.g., [7]) or removing any responsibility for security from the user. However, the latter will only provide some level of security when the system can indeed protect against eventuality, which is unlikely given the use of mobile devices and policies such as BYOD (bring-your-own-devices) being adopted in the workplace. A healthy combination of both seems more appropriate.

How do we better consider the context when individuals make decisions?

You may share a password with a partner, to build trust but you wouldn't share with anyone else. The sensitivity of personal data, such as about one's health, also influences privacy concern [2]. In a similar fashion, so does poor health status [2]. So context is important, both in terms of the information and the situation individuals face.

Based on our research and that of previous uses on mobile devices [4], we would like to suggest that individuals perform different behaviours on their devices depending on their ownership of the devices (employer- or privately owned), the function of the computers as primary or secondary devices, the role of costs and financial incentives. Some behaviour may be perceived as representing a greater risk to privacy than others (e.g., banking vs. social networking). Another question therefore: To what extent then are some behaviour more closely linked to privacy concerns than others? Discussing these findings and questions with workshop collaborators may help us develop a tool kit to consider which variables we need to control for/ evaluate as well when examining the privacy-behaviour link.

To what is the popularity of personalization undermining privacy protective motives?

Personalized websites, computers, user interfaces and applications are increasingly popular. Not only do they cater to the needs of the person using these technological options, but they may also make it easier for them to obtain and structure information. Yet at the same time, these personalization options may increase the risk that users are no longer fully in control of their data. In addition, such personalization may even "amplify and complicate the Internet's inherent privacy risks and concerns" [23], an assessment we agree with. Turning back the clock on personalized services is unlikely to be successful, but we do need to consider the possibility of devices platform and application independent cross-functional privacy systems that will detect potential privacy risks that may result due to personalization preferences.

Where do we draw the line between organizational and individual privacy practices? Is there a line?

The discussion of responsibility for appropriate privacy behaviours can be attributed to either two parties, or shared equally. Evidence suggests that privacy practices are not necessarily seen as part parcel of organizational corporate responsibility, as a result evidence supporting the institutionalization of appropriate evidence is rare [22]. If organizations take the lead, will this increase employee/ individual awareness of appropriate privacy practices? Starting a discussion about the various stakeholders that need to be

consulted and involved in the development of privacy practices may increase awareness for this issue at both organizational and individual levels of action.

6. ACKNOWLEDGMENTS

We would gratefully acknowledge the support and the contribution of our colleagues from Computing Science at Newcastle University who worked with us. This research is supported by EPSRC Grant EP/K006568 Choice Architecture for Information Security, part of the GCHQ/EPSRC Research Institute in Science of Cyber Security.

7. REFERENCES

[1] Altman, J. The environment and social behaviour: privacy, personal space, territory and crowding. Brooks/Cole Publishers, 1975.

[2] Bansal, G., Zahedi, F.M., and Gefen, D. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems 49* (2010), 138-150.

[3] Buchanan, T., Paine, C., Joinson, A.N., and Reips, U.-R. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology, 58*, 2 (2007), 157-165.

[4] Chin, E., Porter Felt, A., Sekar, V., and Wagner, D. Measuring user confidence in smartphone security and privacy. *Proc. SOUPS* (Symposium on Usable Privacy and Security) (2012), 1-16.

[5] Clarke, R. Vignettes of corporate privacy disasters. (accessed April 11, 2014) http://www.rogerclarke.com/DV/PrivCorp.html.

[6] Drennan, J., Sullivan, G., and Previte, J. Privacy, risk perception, and expert online behavior: An exploratory study of household end users. *Journal of Organizational and End User Computing, 18*, 1 (2006), 1-22. DOI=10.4018/joeuc.2006010101.

[7] Furnell, S., Tsaganidi, V., and Phippen, A. 2008. Security beliefs and barriers for novice Internet users. *Computers & Security 27* (2008), 235-240.

[8] Garfinkel, D. *Database Nation: The death of privacy in the 21st Century*. CA: O' Reilly Media, 2001.

[9] Han, J., and Kamber, M. *Data Mining: Concepts and Techniques*. Morgan Kaufmann, 2000.

[10] Hough, M. G. Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society, 31*, 4 (2009), 406-413.

[11] Hugl, U. Reviewing person's value of privacy of online social networking. *Internet Research, 21*, 4 (2011), 384-407.

[12] Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security, 31* (2012), 83-95.

[13] Jensen, C., Potts, C., and Jensen, C. Privacy practices of Internet users: Self-report versus observed behavior. *International Journal of Human-Computer Studies, 63* (2005), 203-227.

[14] Joinson, A. N., and Paine, C. B. Self-disclosure, privacy and the Internet. In *Oxford Handbook of Internet Psychology*, no. 1971, A. Joinson, K. McKenna, T. Postmes, and U.-D. Reips, Eds. Oxford University Press, 237-252, 2007.

[15] King, J., Lampinen, A., and Smolen, A. Privacy: Is There An App for That? *Proc. SOUPS* (Symposium On Usable Privacy and Security) (2011), 1-20.

[16] Kurkovsky, S., and Syta, E. Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. *Proc. ISTAS* (International Symposium of the Technology and Society) (2010), 441 – 449.

[17] Lacohee, H., Phippen, A.D., and Furnell, S.M. Risk and restitution: Assessing how users establish online trust. *Computers & Security 25* (2006), 486-493.

[18] Li, Y. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems 54* (2012), 471-481.

[19] Metzger, M.J. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication 9,* 4 (2006), 1-29.

[20] Newell, P. B. A systems model of privacy. *Journal of Environmental Psychology* 14, 1 (1994), 65-78.

[21] Pedersen, D.M. Model for types of privacy by privacy functions. *Journal of Environmental Psychology 19* (1999), 397-405.

[22] Pollach, I. Online privacy as a corporate social responsibility: An empirical study. *Business Ethics: A European Review 20*, 1 (2011), 88-102.

[23] Toch, E., Wang, Y., and Cranor, L.F. Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems. *User Modelling and User-Adaptive Interaction 22* (2012), 203-220.

[24] Tsai, J.Y., Egelman, S., Cranor, L., and Acquisti, A. The effect of online privacy information on purchasing behaviorL An experimental study. *Information Systems Research 22*, 2 (2011), 254-268.

[25] Ward, J. H. Hierarchical Grouping to Optimize an Objective Function. *Journal of the American Statistical Association, 58*, 301 (1963), 236-244.

[26] Westin, A. *Privacy and Freedom*. New York: Atheneum, 1967.

[27] Wu, K.-W., Huan, S.Y., Yen, D.C., and Popova, I. The effect of online privacy policy on consumer policy concern and trust. *Computers in Human Behavior 28* (2012), 889-897.